Attribution in Cryptocurrency Cases

Michele R. Korver
Digital Currency Counsel
Criminal Division
Money Laundering & Asset Recovery Section
United States Department of Justice

C. Alden Pelker
Trial Attorney
Criminal Division
Computer Crime and Intellectual Property Section
United States Department of Justice

Elisabeth Poteat
Trial Attorney
National Security Division
Counterterrorism Section
United States Department of Justice

It is possible to develop attribution in cases involving cryptocurrency despite the fact that these transactions are generally considered anonymous. Prosecutors should anticipate that a constellation of information will have to be developed, not a simple chain. In cryptocurrency cases there is not a particular company with custody of the evidence that can be served.

Throughout this piece the authors use the words "coins," "cryptocurrency," and "virtual currency" interchangeably to describe any non-fiat currency on a blockchain.

I. Introduction

A. Cryptocurrency overview

Developing attribution is a challenge because of the way cryptocurrency functions. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer network-based medium of value or exchange. Cryptocurrency may be used as a substitute for government-backed "fiat" currency to buy goods or services, or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer

cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object, the recovery of which can assist in development of attribution. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether, but there are hundreds as of this writing.

Most cryptocurrencies have a blockchain, which is a distributed public ledger containing an immutable and historical record of every transaction.[1] Using open source or subscription analytical tools, cryptocurrency transactions can often be traced in their blockchains. Some cryptocurrencies, however, operate on blockchains that are not public. They may operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions. The blockchain information itself is a single data point, albeit an important one, in the overall attribution picture.

Cryptocurrency can be accessed through a virtual account of sorts called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. In the cryptocurrency realm, a public key or address is roughly akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. The location and recovery of a private key, in whatever format it may be found, is highly valuable to attribution.

Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet based cloud storage provider ("online wallet"), as a mobile application on a smartphone ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange.[2]

When drafting affidavits, pleadings, and jury instructions in cases involving this technology, prosecutors should recognize the need to educate judges and jurors on basic terms and concepts underlying cryptocurrencies and blockchains. In particular, in explaining the

---

[1] Commodity Futures Trading Comm'n v. McDonnell, 287 F. Supp. 3d 213, 218–19 (E.D.N.Y. 2018).

[2] *See id.*

places or persons to be searched, physical or virtual, the prosecutor should focus on explaining what a private key is, where it might be located, the forms it might take, and the possibility or likelihood that it might be in an encrypted format or held in a cipher.

B. Existing primers

There is no substitute for understanding blockchain technology at the earliest stages of the investigation in order to guide the development of attribution. Prosecutors can familiarize themselves with virtual currency and better understand how it is exploited for unlawful purposes. There are also several websites that publish frequent updates to news on virtual currency, as well as primers prepared by virtual currency specialists. The websites and primers may be helpful to better understanding the technology and legal landscape. Many public websites collect viewer data, so prosecutors should be cautious as they navigate these sites.

1. Prior bulletins, anticipated bulletins, and what we do not repeat

The authors recommend Assistant United States Attorney Matthew J. Cronin's primer, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*,[3] which appeared in the Department of Justice Journal of Federal Law and Practice (formerly USA Bulletin) in July 2018. This article discusses some of the pitfalls of conducting an investigation that reaches into the darknet, and presents practice suggestions upon which the authors herein seek to expand.

The authors encourage readers to review other pieces and their explanations of the importance of searching for private keys in physical searches of homes or searches of accounts held by electronic communications providers; records of deposits into traditional financial institutions close in time and in an amount consistent with known illicit cryptocurrency transactions; searches of computer logs for records of activity including Tor links, exchanges, and mixers/tumblers; and background material on the cryptocurrencies used or the illicit items/information involved in the underlying crime. The authors concur with their colleagues who have emphasized the importance of leveraging in-person interviews to acquire information, while at the same time cautioning that interviews can also prompt the destruction of evidence (both physical and virtual) or raise issues of

[3] 66 U.S. ATT'YS BULL., no. 4, 2018, at 65–78.

parallel civil and criminal proceedings. These include, but are not limited to, overlapping criminal and civil discovery issues and statements taken by regulatory agents, some of whom are category 1811 sworn federal agents, who may be aware of ongoing criminal investigations or grand jury material.[4]

2. Coin Center, Brito primer, and Coindesk.com

Coin Center is a non-profit and advocacy center that focusses on cryptocurrency policy issues.[5] The Executive Director of Coin Center is Jerry Brito. Brito authored *Bitcoin: A Primer for Policymakers*.[6]

CoinDesk is a website that offers cryptocurrency news by what it bills as a group of independent journalists.[7] CoinDesk was founded by cryptocurrency investor Shakil Khan. The website posts the Bitcoin Price Index, which, according to CoinDesk's Wikipedia page, is referenced occasionally by Bloomberg.[8]

3. More information in public domain can cause attribution blues

On July 13, 2018, a grand jury in the Federal District Court for the District of Columbia returned an indictment against 12 Russians alleged to have engaged in large-scale cyber operations in an effort to interfere with the 2016 U.S. presidential election.[9] Count ten of the indictment set forth the way in which the group used cryptocurrency to cover its tracks.[10] Instead of just receiving cryptocurrency as payment for illicit narcotics, weapons, or child pornography, the group members took a different approach. They used cryptocurrency to buy infrastructure to be used to hack computers and to register domains.[11] They tried a familiar technique of using hundreds of different email accounts and even mining bitcoin, a process that requires a significant

---

[4] *See* JUSTICE MANUAL § 1-12.000; ORG. AND FUNCTIONS MANUAL § 27.
[5] *See* COIN CENTER, https://coincenter.org/ (last visited Oct. 22, 2018).
[6] JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS (2d ed. 2016).
[7] COINDESK, www.coindesk.com (last visited Oct. 22, 2018).
[8] *CoinDesk*, WIKIPEDIA, https://en.wikipedia.org/wiki/CoinDesk (last visited Oct. 22, 2018).
[9] Indictment, United Sates v. Viktor Borisovich Netyksho et al., No. 1:18-cr-00215-ABJ (D.D.C. July 13, 2018), ECF No. 1.
[10] *Id.* at ¶¶ 56–64.
[11] *Id.*

amount of computing power.[12] The "speaking indictment" in the case sets forth a detailed account of how the conspirators were ultimately identified despite their efforts at obfuscation.[13]

In August of 2018, following the indictment, Nick Furneaux, a cyber-security consultant in the United Kingdom, published a detailed book on how to investigate cryptocurrencies.[14]

4. Staying current in a rapidly shifting terrain

There may be no substitute for staying current for prosecutors working on cases involving cryptocurrencies. Prosecutors frequently encountering cryptocurrency-related cases may consider setting Westlaw, Lexis, and Google Scholar alerts to remain aware of published materials and news on cryptocurrency. Of course, reaching out to colleagues who have handled recent cases with cryptocurrency is a tried-and-true way to gain expertise, and is consistent with the esprit de corps that exists among prosecutors in the Department of Justice. Both the Computer Crime and Intellectual Property Section (CCIPS) and the Money Laundering and Asset Recovery Section (MLARS) have attorneys who possess subject matter expertise in cryptocurrency, and there are a number of Assistant United States Attorneys around the country who are well-versed in cryptocurrency matters. Prosecutors should avail themselves of these resources whenever confronting a cryptocurrency related case.

C. Applicable regulations and laws

1. Criminal code violations

There is a range of criminal activity which may involve or be facilitated by cryptocurrencies. The activity will inform where investigators should look for attribution and how it is developed.

Cryptocurrencies are generally used in two ways: (1) as a tool or technique to transfer or store value and (2) to acquire the tools necessary to commit certain crimes, such as weapons or toxins for crimes of violence, servers and domains used for hacking, or conducting malign influence campaigns and more. Thus, established

---

[12] *Id.*

[13] *Id.*

[14] NICK FURNEAUX, INVESTIGATING CRYPTOCURRENCIES: UNDERSTANDING, EXTRACTING, AND ANALYZING BLOCKCHAIN EVIDENCE (David S. Hoelzer ed., 1st ed. 2018).

criminal statutes work well as charging options.

Often cryptocurrencies are used as the preferred payment method for distribution of contraband and other illegal goods and services, or as a means of collecting funds from victims of traditional fraud or computer intrusions, such as ransomware. This means that a wide variety of offenses punishable under Title 18, including wire fraud, mail fraud, access device fraud and identity theft, and fraud in connection with computers,[15] as well as contraband type violations such as illegal firearms sales and possession,[16] possession or distribution of counterfeit items,[17] and offenses punishable under Title 21 United States Code are possible.

Focusing on the cryptocurrency transactions, prosecutors have a wide variety of money laundering violations at their disposal. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering pursuant to 18 U.S.C. § 1956,[18] or qualify as a monetary transaction involving proceeds of illegal activity under section 1957.[19] In addition, individuals or companies engaged in money transmission involving cryptocurrency may be subject to state and federal registration, and record keeping and reporting requirements punishable under 18 U.S.C. § 1960[20] and Title 31,[21] as further discussed below. Moreover, cryptocurrency transactions may be used as the means to collect funds relating to terrorist financing,[22] pay for acts of espionage under Title 18, Chapter 37,[23] conduct foreign influence campaigns or criminal violations of the Foreign Agents' Registration Act,[24] support of child exploitation activities under Title

---

[15] 18 U.S.C. §§ 1343 (wire fraud), 1341 (mail fraud), 1029 (access device fraud), 1028 (identity theft and fraud), 1028A (aggravated identify theft), and 1030 (fraud in connection with computers).
[16] 18 U.S.C. § 921 *et seq*.
[17] 18 U.S.C. § 2320.
[18] 18 U.S.C. § 1956.
[19] § 1957.
[20] § 1960.
[21] 31 U.S.C. § 101 *et seq*.
[22] 18 U.S.C. § 2339 *et seq*.
[23] 18 U.S.C. § 792 *et seq*.
[24] 22 U.S.C. § 611 *et seq*.

18, Chapter 110,[25] or engage in computer intrusion activities.[26]

Finally, as with any illegal activity involving some form of financial transaction or concealment, prosecutors should consider tax violations where appropriate.

2. FinCEN and the Bank Secrecy Act

Some exchanges function as regulated businesses, which may hold information valuable for attribution. The Department of Treasury's Financial Crimes Enforcement Network (FinCEN) has primary responsibility for administering the Bank Secrecy Act (BSA)[27] and implementing its regulations. Perhaps most important for attribution development, FinCEN is the steward of the BSA database.[28]

FinCEN regulates individuals or entities engaged in the business of accepting and transmitting virtual currency. FinCEN requires money services businesses (MSBs) that conduct money transmission in virtual currency to meet the same AML/CFT[29] standards as other money services businesses under the BSA.[30] This includes registering with FinCEN, establishing an AML program reasonably designed to prevent money laundering and terrorist financing, and meeting certain recordkeeping and reporting obligations, such as filing Suspicious Activity Reports (SARs).[31] FinCEN also collects foreign bank account reports (FBARs), currency and monetary instrument reports (CMIRs), and currency transactions reports (CTRs)—all of which contain pieces of information that may be used to develop attribution.[32]

SARs are lead information only and are generally inadmissible in court.[33] A target or subject cannot be told about the existence of a SAR

---

[25] 18 U.S.C. § 2251 *et seq*.
[26] 18 U.S.C. § 1030.
[27] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970).
[28] *See* 31 U.S.C. § 310(c).
[29] U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, ADVISORY ON THE FATF-IDENTIFIED JURISDICTIONS WITH AML/CFT DEFICIENCIES (Apr. 2018) (defining AML as anti-money laundering and CFT as combatting the financing of terrorism).
[30] *See* 31 U.S.C. § 5330.
[31] 31 C.F.R. §§ 1010.300 *et seq*.
[32] 31 C.F.R. §§ 1010.300–1010.370.
[33] *See, e.g.,* Weil v. Long Island Savings Bank, 195 F. Supp. 2d 383, 389 (E.D.N.Y. 2001).

by anyone during an interview intended to develop attribution.[34] Law enforcement agents are permitted, however, to request supporting documents evidencing the suspicious activity or transaction from a financial institution, and thereafter develop a more fulsome record of the cryptocurrency use or formulate questions that avoid referencing any SAR.[35] FinCEN's requirements apply equally to domestic and foreign located virtual currency money transmitters—even if the foreign located entity does not have a physical presence in the United States.[36] The entity need only do business, in whole or substantial part, in the United States.[37]

In 2011, FinCEN issued a final rule that, among other things, defined "money transmission services" to include accepting and transmitting "currency, funds, or other value that substitutes for currency . . . by any means."[38] The phrase "other value that substitutes for currency" is intended to encompass situations when a transmission includes something that the parties recognize has value, which is equivalent to, or can substitute for, real currency. The definition of "money transmission" is technology neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another person or from one location to another location is regulated under the BSA.[39]

In March 2013, to provide additional clarity and respond to questions from the private sector, FinCEN issued interpretive guidance regarding the application of FinCEN's regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency (hereinafter the 2013 Guidance).[40]

The 2013 Guidance identified the participants to some virtual currency arrangements, including "exchangers," "administrators," and "users," and clarified that exchangers and administrators generally qualify as money transmitters under the BSA, but users do not.[41] The 2013 Guidance states that virtual currency administrators and

---

[34] 31 U.S.C. § 5318(g)(2)(A)(ii); 75 Treas. Reg. § 75593-01 (2010).
[35] 31 C.F.R. § 1010.320(d).
[36] Kenneth A. Blanco, FinCEN Dir., Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018).
[37] *Id.*
[38] 76 Treas. Reg. § 43585-01.
[39] *Id.*
[40] Press Release, Fin. Crimes Enf't Network, FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities (Mar. 18, 2013).
[41] *Id.*

exchangers, including an individual exchanger operating as a business, are considered MSBs, obligated to have AML programs, and file SARs or other BSA reports.[42]

FinCEN has issued several administrative rulings providing additional clarity regarding virtual currency matters including, but not limited to, discussing virtual currency issues such as mining and operating a virtual currency trading platform.[43] In an August 9, 2018 public statement of its Director, FinCEN advised that its regulations cover transactions where the parties are exchanging fiat (meaning issued by a government or nation) and convertible virtual currency, and transactions from one virtual currency to another virtual currency.[44]

If there is an MSB involved in the case, a prosecutor can begin to look for attribution information in reports within the FinCEN database.[45] Prosecutors should keep in mind any legal restrictions on the use of the information as they develop their attribution.

3. Office of Foreign Assets Control

Cryptocurrency moves globally, and in some instances it moves to countries under U.S. State Department (State) or Treasury sanctions. The Office of Foreign Assets Control (OFAC) of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries and regimes; terrorists; international narcotics traffickers; those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to the national security, foreign policy, or economy of the United States based on U.S. foreign policy and national security goals.[46]

---

[42] *See* U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (Mar. 18, 2013).

[43] *See* FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/ (last visited Nov. 13, 2018).

[44] Kenneth A. Blanco, FinCEN Dir., Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018).

[45] *See* FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/ (last visited Nov. 13, 2018).

[46] *See Office of Foreign Assets Control—Sanctions Programs and Information,* U.S. DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (last visited Oct. 22, 2018).

OFAC compliance obligations are the same for individuals transacting in digital currency. As a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment related transactions.[47] Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities.[48] Additionally, persons who provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority. This includes technology companies, administrators, exchangers, and users of digital currencies.[49]

In any case involving cryptocurrency, there could be attribution information within OFAC's holdings that may be part of an administrative record. Portions thereof may be classified for reasons of national security. The parallel proceedings concerns with using this information are the same as with other regulatory agencies' holdings. Prosecutors should carefully consider each concern before contacting OFAC for attribution information. Both MLARS and the National Security Division (NSD) can be helpful to addressing these concerns. NSD can provide guidance on the considerable legal restrictions on classified information.

4. SEC and securities

In 2017, the Securities and Exchange Commission (SEC) issued an investigative report cautioning market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of the federal securities laws.[50] Such offers and sales,

---

[47] *Resource Center, OFAC FAQs: Sanctions Compliance*, U.S. DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx (last visited Dec. 4, 2018).

[48] *Id.*

[49] *Id.*

[50] U.S. Sec. & Exch. Comm'n, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Release No. 81207, July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

conducted by organizations using distributed ledger or blockchain technology, have been referred to, among other things, as "Initial Coin Offerings" (ICOs) or "Token Sales."[51] "Whether or not a particular transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction."[52]

The SEC has suspended trading of more than a dozen common stocks of certain issuers who made claims regarding their investments in ICOs or touted coin/token related news. It has warned investors about potential scams involving companies claiming to be related to, or asserting they are engaging in, ICOs. Parties perpetrating these scams often use the lure of new and emerging technologies to convince potential victims to invest.

Public statements regarding registration or principals engaged in offerings may assist in establishing attribution in cases where ICOs are launched for the purpose of facilitating or covering up criminal activity. But if the SEC is conducting an investigation or enforcement action, prosecutors may encounter parallel proceedings issues, such as restrictions on the use of statements made by a target to the SEC coterminous with a criminal case that was not public. This can complicate any efforts to use SEC-acquired information to help establish attribution and should be carefully considered.[53] SEC staff providing assistance on these matters can be reached at FinTech@sec.gov.

5. Commodity Futures Trading Commission and Commodities Trading

Like FinCEN, the Commodity Futures Trading Commission (CFTC) regulates certain uses of cryptocurrency and may be a source of information that can be used to develop attribution. The CFTC has oversight over futures, options, and derivatives contracts under the Commodity Exchange Act (CEA).[54] The CFTC declared virtual currencies can be "commodities" subject to oversight under its CEA authority.[55] The CEA definition of commodity includes "all services,

---

[51] *Id.* at 1.
[52] *Id.* at pp.16–17.
[53] *See* JUSTICE MANUAL § 1-12.000.
[54] 7 U.S.C. § 1 *et seq.*
[55] Commodity Futures Trading Comm'n v. McDonnell, 287 F.3d 213,

rights, and interests in which contracts for future delivery are presently or in the future dealt in."[56]

The CFTC's jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce. In its regulatory role, the CFTC has taken action against unregistered bitcoin futures exchanges; enforced laws prohibiting wash trading[57] and prearranged trades on a derivatives platform; issued proposed guidance defining derivative and spot markets in the virtual currency context; issued warnings about valuations and volatility in spot virtual currency markets; and addressed a virtual currency Ponzi scheme.

"Beyond instances of fraud or manipulation, the CFTC generally does not oversee 'spot' or cash market exchanges and transactions involving virtual currencies which do not utilize margin, leverage, or financing."[58] Aspects of the CFTC's enforcement actions, however, are public and can be mined for attribution information, provided prosecutors do not run afoul of parallel proceedings restrictions.

6. IRS and tax enforcement

According to the Internal Revenue Service (IRS), virtual currency transactions, like any other property transactions, are taxable as

---

228 (E.D.N.Y. 2018); Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions at 3, *In re* Coinflip, Inc., No. 15-29 (Commodity Futures Trading Comm'n Sep. 17, 2015), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf ("Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.").

[56] *CFTC Glossary*, U.S. COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/glossary_co.html (last visited Nov. 12, 2018) (defining commodity).

[57] *CFTC Glossary*, U.S. COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/glossary_wxyz.html (last visited Nov. 12, 2018) ("Wash trading" is defined as "Entering into, or purporting to enter into, transactions to give the appearance that purchases and sales have been made, without incurring market risk or changing the trader's market position.").

[58] LABCFTC, A CFTC PRIMER ON VIRTUAL CURRENCIES 11 (Oct. 17, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf.

income.[59] The IRS has concluded that virtual currency will be treated as property for U.S. federal tax purposes, which means that a payment in virtual currency is subject to information reporting just like any other payment in property. Further, third parties who settle payments made in currency on behalf of merchants accepting virtual currency must report those payments to the IRS, among other things. That can mean that the IRS has within its holdings a small piece toward attribution.

A court order for tax returns may lead to evidence of attribution, mens rea, or may suggest tax related charges in any case involving cryptocurrency.

II. Before you develop attribution

A. De-conflicting

Law enforcement agents conducting undercover investigations involving cryptocurrency related entities in the darknet need to ensure that they are not investigating the same subjects as other agencies. They should also take steps to ensure they are not communicating with other law enforcement agents posing as criminals. Before conducting undercover operations, prosecutors should make sure that law enforcement agents have checked with appropriate multi-agency de-confliction organizations and databases. This should be done in any routine undercover case that may involve cryptocurrency.

In addition, as investigators develop bits of attribution evidence in their cases, such as email addresses, online usernames, or cryptocurrency public addresses, they should continually enter the information in the de-confliction databases to avoid conflicts while the case is ongoing.

B. Discussing investigative agents and analysts' compliance with their agencies' policies and procedures

The proper documentation of the forensic trail used by investigators will be important to showing why the government's assessment of attribution is reliable. Documentation should start early. Prosecutors can avoid the creation of a weak audit trail by following some basic common sense principles. First, investigator access to the darknet

[59] INTERNAL REVENUE SERV., NOTICE 2014–21 (2014).

should not be undertaken except through the use of techniques that have been approved by their agency.

All federal law enforcement agencies have policies and procedures governing undercover activities. Many are contained within larger general orders and updated on a regular basis, such as the FBI's Domestic Investigative and Operations Guide.[60] In addition, the agency may have other guidance or policy governing undercover operations in cyberspace, in particular the darknet.

An investigative agency's written policies on Tor access or undercover cyber operations should be followed unless technologically obsolete and there is a memorialized consensus within the agency's leadership about its obsolescence. Prosecutors should document law enforcement work that may appear to be a policy deviation and be prepared to have a witness explain it in court. Any deviation from the policies may complicate undercover operations, compromise the investigation, or become an issue at trial, particularly for attribution. No attribution should appear flawed because of a failure to follow agency rules.

III. Blockchain analysis's role in attribution

Cryptocurrencies rely on "blockchains," in which transactions are memorialized after they have been cryptographically signed and verified. Many cryptocurrencies have public blockchains allowing anyone to view the full history of transactions for every cryptocurrency address involved in a transaction. The blockchain thereby serves as a public transaction ledger and an incredibly valuable resource for investigators. Armed only with the knowledge of a target's cryptocurrency address and this single—but highly valuable—data set, law enforcement can learn a myriad of vital pieces of information about a target. For example, the blockchain can reveal the total amount that the subject sent and received, the total value of the subject's current holdings in the cryptocurrency, the addresses to which the subject sent funds, the addresses from which the subject received funds, and the addresses of co-conspirators and other

---

[60] *FBI Domestic Investigations and Operations Guide*, FED. BUREAU OF INVESTIGATION, https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 (last visited Nov. 14, 2018).

associated individuals. Blockchain analysis can even show incoming transactions from victims. These transactions may reveal the number of victims and the amount of money received from the victims, as well as the victims' cryptocurrency addresses. The addresses may assist with identifying and notifying victims of a wide range of criminal schemes.

While this information can be highly valuable to a criminal investigation, the value largely depends on the investigators' ability to put the information into context. On its own, viewing cryptocurrency transactions on the blockchain shows only the transfer of some quantity of funds from one string of letters and numbers to another at a point in time. Correlating that activity to real world events—for example, the payment of funds by a victim or an undercover agent—provides additional context. The greatest value, however, may come from the ability to associate certain addresses with known entities, particularly virtual currency exchanges. The known entities may collect records regarding the user's true identity and by tracing a target's funds to the entity, law enforcement can glean valuable insight into a target's true identity.

A. Commercial tools and clustering

Law enforcement uses commercial services offered by several different blockchain analysis companies to investigate certain types of cryptocurrency transactions, most frequently Bitcoin. These companies analyze the blockchain in an attempt to identify the individuals or groups involved in the cryptocurrency transactions. In addition to its use by law enforcement, this third-party blockchain analysis software is used as anti-money laundering software by financial institutions worldwide.

One feature of the software that is particularly valuable to law enforcement is "clustering." Many cryptocurrency users set up multiple addresses. For example, a user or business may create many cryptocurrency addresses to receive payments from different customers. When the user wants to move the cryptocurrency received (for example, to exchange one type of cryptocurrency for other currency or to use cryptocurrency to purchase goods or services), it may group those addresses together to send a single transaction. Because only the user holding an address' private key can spend funds associated with that address, the user responsible for a transaction spending funds from multiple cryptocurrency addresses must have the private key associated with each of the addresses.

For law enforcement, it is highly valuable to be able to accurately associate multiple addresses to a given individual or entity. Law enforcement uses third-party blockchain analysis software to locate cryptocurrency addresses that are spent together in a single transaction. These addresses can then be "clustered" together to represent the same owner. The clusters associated with major darknet marketplaces can amass tens of thousands of addresses.

Several sites offer free, basic blockchain analysis tools that allow users to view the transaction history associated with a given address. While these tools may allow the user to perform some basic tracing, they unfortunately are often insufficient for tracing or attributing complex fund flows.

B. Legal considerations

Before using commercially available tools for forensics or blockchain analysis, consider how the prosecution will lay a foundation for the reliability of the tools for a judge or jury. While many of these tools are in the public domain, they will still have to be explained to a fact finder. Anticipate that proprietary algorithms or other trade secrets may also be used in commercial tools. Trade secrets may need to be protected from public disclosure through a motion for a protective order. Prosecutors should consider consulting with CCIPS when they face any trade secrets issues in an investigation.

If any blockchain analysis relies upon a commercial tool, there may be limitations to the licensing of that tool to the federal government agency. An attorney from the agency's general counsel's office will likely know if there are any limitations based on the contract between the law enforcement agency and the private company.

C. Acquiring information from exchanges

Since the blockchain serves as a searchable public ledger of every cryptocurrency transaction, investigators may trace transactions to cryptocurrency exchanges. Because those exchanges collect identifying information about their customers, subpoenas or other appropriate process submitted to the exchanges can, in some instances, reveal the true identity of the individual responsible for the transaction. In the United States, exchanges are considered MSBs which must register with FinCEN and collect "Know Your Customer," commonly referred

to as "KYC," information.[61] These FinCEN registered exchanges may hold valuable information, including: the target's true name; date of birth; driver's license; passport and/or social security number; bank account information; e-mail address; phone number; IP address and device information; photograph; transaction history; and information pertaining to other services used by the target. Many exchanges operating outside of the United States also collect this type of information.[62]

For U.S.-based virtual currency exchanges, prosecutors and investigators can obtain records using a grand jury subpoena. Foreign-based virtual currency exchanges servicing U.S. customers or otherwise doing business in the U.S. are required to have a U.S. agent for receiving process.[63]

If the exchange is overseas without a U.S. presence, records can be obtained via Mutual Legal Assistance Treaty (MLAT). The case agent may also consider submitting an EGMONT request through FinCEN,[64] but it comes with possible limitations.[65] These requests are received by the Financial Intelligence Units (FIUs) of foreign countries, some of which lack the power to produce records exceeding those comparable to SARs under the BSA.[66] Moreover, an FIU may be obligated to share a request with their law enforcement or intelligence counterparts, thereby potentially compromising an ongoing investigation. An EGMONT response may come with conditions,

---

[61] Guidance FIN-2013-G001 from Dep't of the Treasury Fin. Crimes Enf't Network on Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[62] Advisory FIN-2012-A001 from Dep't of the Treasury Fin. Crimes Enf't Network on Foreign-Located Money Services Businesses (Feb. 15, 2012), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a001.

[63] *Id.*

[64] *See* EGMONT GROUP, https://www.egmontgroup.org/ (last visited Nov. 14, 2018).

[65] Case agents may also work through their relevant law enforcement agency's liaison seated at FinCEN for submitting EGMONT requests.

[66] While the EGMONT principles of information exchange may encourage sharing rules that are consistent, individual nations are still subject to the laws within their sovereign territories. EGMONT Group of Financial Intelligence Units Charter, Oct. 30, 2013.

including limitations on the use of the information received.

Records from the exchanges alone, however, may be insufficient. Many exchanges, particularly those located outside of the United States or whose operators do not comply with U.S. Bank Secrecy Act requirements, may collect nothing more than an email address from their account holders and perform little to no identity verification. More sophisticated individuals will likely avoid using the exchanges that collect identification information in an effort to avoid detection and attribution of transactions by law enforcement. Prosecutors should nonetheless attempt to collect evidence from established exchanges or seized data sets of shut down exchanges.

Finally, statutory non-disclosure requirements do not apply to cryptocurrency exchanges (MSBs) and related companies in the same manner as for traditional financial institutions or internet service providers.[67] Some entities value customers' absolute privacy and pseudo anonymity—two goals that have motivated the development of many cryptocurrencies—more than compliance with government requests and AML/CFT concerns. Prosecutors should be aware that cryptocurrency service providers may disclose to customers the fact of receipt of a law enforcement request for information, despite the fact that such disclosures are not a legitimate practice.

Prosecutors are strongly encouraged to work through the appropriate main Department of Justice component to become aware of the risks that may be presented and to help manage expectations of the prosecution and investigative teams.

D. Blockchain obfuscation techniques (chain-hopping/tumblers/mixers)

Criminals are actively seeking to frustrate law enforcement's ability to effectively trace transactions on the blockchain. One common technique involves the use of a cryptocurrency "mixer" or "tumbler." The mixer or tumbler may operate as a stand-alone service or may be integrated into some other service, such as a darknet marketplace.

Mixers attempt to obfuscate the source or owner of cryptocurrency by mixing the cryptocurrency of several users prior to delivery to its ultimate destination. Mixers, for a fee, allow users to conceal proceeds from illegal transactions by accepting "dirty" bitcoins[68] from users and

---

[67] *See* 18 U.S.C. § 1510(b); 18 U.S.C. § 2703(d).

[68] "Dirty" bitcoins are cryptocurrency used in furtherance of illegal activities,

returning "clean" bitcoins[69] to a wallet address specified by the original user. Different mixers have various features and processes. Generally, the customer can send cryptocurrency to a specific wallet address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers and sends it through a convoluted series of transactions, making it difficult to track on the blockchain. When a customer makes a request to "cash out" his or her cryptocurrency, the mixer arranges for the funds to be transferred from another address that cannot be traced to the customer.

Criminals also engage in a practice known as "chain hopping," in which they move from one cryptocurrency to another, often in rapid succession. Because each cryptocurrency has its own blockchain, investigators who are trying to follow these trails may encounter significant difficulties. Depending on the service through which the target exchanged the original form of cryptocurrency for another cryptocurrency, it may be difficult to determine if and when a chain hop has occurred. This difficulty is exacerbated by the difficulty in tracing certain alternative coins, particularly those that do not have a public blockchain.

E. Cautions

Cryptocurrency cases can certainly challenge a prosecutor's ability to anticipate risks in any investigation. The topography of cryptocurrency cases may seem marked by sudden deep chasms. The places where information of attribution might be sought are not always like traditional financial institutions that have a robust legal compliance shop. Evidence is often held in countries with which the United States has uneven relationships.

Many wallet hosting services are located outside of the United States. Prosecutors should consult with the Office of International Affairs (OIA) prior to engaging in activities which may require access to servers or companies located internationally. Some activities may require an MLAT or other similar authority even where the wallet company does not itself have access to or control of the cryptocurrency accounts.

---

such as those taking place on Darknet marketplaces.

[69] "Clean" bitcoins are bitcoins that purportedly cannot be traced to illegal activities.

National security issues can arise in cryptocurrency cases after the investigation is underway. The issues may prompt concerns that there may be classified information related to the case in the possession of the intelligence community agencies. Classified information in a case is often identified through a response to a Prudential Search Request (PSR).[70] PSRs are simply written requests to intelligence agencies[71] to search their holdings for information related to a particular case. If prosecutors or the law enforcement agent assigned to the case have a specific reason to believe that the intelligence community may be in possession of information that relates to the case, a PSR should be a part of a prosecutor's due diligence efforts. All PSRs must be sent to the NSD. NSD's Counterterrorism and Counterintelligence and Export Control Sections are the points of contact for PSRs in counterterrorism and counterintelligence cases, and the Law and Policy Section for all other criminal cases.[72] All PSRs directed to the intelligence agencies, however, must come from NSD. NSD attorneys will assist with these requests.[73]

Where national security charges are contemplated, prosecutors should consult with their national security sections, their Antiterrorism Coordinators, and adhere to the Department of Justice policies set forth in Title 9 of the Justice Manual,[74] and other Department of Justice policies governing national security cases. NSD prosecutors have expertise in managing classified information and the Classified Information Procedures Act.[75]

---

[70] *See* CRIM. RESOURCE MANUAL § 2052 (defining "prudential search").
[71] *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 1011 (codified as 50 U.S.C. § 3003(4)) (identifying intelligence agencies).
[72] JUSTICE MANUAL § 9-90.200; Memorandum from Gary G. Grindler, Acting Deputy Att'y Gen., U.S. Dep't of Just. on Policy and Procedures Regarding Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations 9–10 (Sept. 29, 2010), redacted version available at Robert Chesney, *Justice Department's 2014 Policy on the Duty to Search for Exculpatory Evidence in IC or DOD Possession*, LAWFARE (Jan. 12, 2018, 8:00 AM), https://www.lawfareblog.com/justice-departments-2014-policy-duty-search-exculpatory-evidence-ic-or-dod-possession [the Grindler Memo].
[73] Grindler Memo, *supra* note 72.
[74] JUSTICE MANUAL § 9-1000 *et seq*.
[75] 18 U.S.C. app. 3.

These concerns may arise as matters of first impression to prosecutors who previously litigated routine criminal cases. Fortunately, the Department of Justice has the right experts to help prosecutors anticipate the risks that could prevent the development of attribution.

IV. Protecting forensic techniques used and managing private companies

In the vast majority of cases, even those involving cryptocurrency, prosecutors will not need to present extensive evidence related to clustering and advanced blockchain analysis. Though those tools may be critical to the initial identification of a target and their assets, investigators often find equally compelling attribution evidence during subsequent investigation. Prosecutors should consider the best way to present their case to the jury, including identification of testimony and evidence that are most helpful.

A. Motions in limine, to seal, for protective order, and other factually specific filings

1. Know about the private company before you plan motions

Many current investigative tools were created by private companies that have received considerable press. Chainalysis, Neutrino, and Elliptic currently provide blockchain analysis services to a variety of customers, while many more companies touting blockchain analysis tools are starting up. Representatives of many of these companies have made public statements or testified before congressional committees about assistance they have rendered to particular agencies or investigations.[76] The executives have also described in

[76] *See, e.g.*, Jonathan Levin, Opening Statement for the House Financial Services Committee's Subcommittee on Terrorism and Illicit Finance (June 8, 2017); Neeraj Agrawal, *Hot Takes*, COINCENTER BLOG (June 30, 2017), https://coincenter.org/link/we-demonstrated-how-bitcoin-works-in-congress; Fortune Staff, *Bitcoin Tracker Chainalysis Raises $16 Million, Plans to Track 10 More Cryptocurrencies*, FORTUNE (Apr. 5, 2018), http://fortune.com/2018/04/05/chainalysis-raises-16m-series-a-plans-to-track-10-more-cryptocurrencies/; Jamie Redman, *Chainalysis Says They've Found the Missing $1.7 Billion Dollar Mt Gox Bitcoins*, BITCOIN.COM (Oct. 15, 2018),

general terms the capacity of their technology to perform analytic tasks (such as clustering), made comments about terrorists' use of virtual currency, and cited to other instances in which they have advised the federal government.

Prosecutors should understand what blockchain analysis tools (or what components of any such tool) are widely known or publicly available, and what are needing of protections as trade secrets or commercial proprietary information. Any discussion with the company providing the tool should take place with an investigative agent present.

2. Motions in limine

Prosecutors may want to file a motion in limine asking the trial court to prevent cross-examination on unrelated classified matters the company may be supporting, on other proprietary information that is not helpful to a defense, or that veers from relevant facts to irrelevant trade secrets. Prosecutors should plan to request the court limit testimony and examination of any witnesses from a private company to facts needed to establish the reliability of the commercial product for attribution or value tracing.

Prosecutors conducting an investigation into a corporation or its leadership may want to determine if the private blockchain analysis company already has a relationship with the corporation under investigation that may present a conflict. This can also avoid surprise to the prosecution at a late stage in the attribution trial.

3. What to place under seal

To avoid actions that could harm the investigation, any affidavit that could signal to a target that an investigation is ongoing or reveal sensitive investigative techniques should be placed under seal. Unsealed affidavits could result in a target fleeing a jurisdiction or avoiding travel to a location where they can be arrested. Further, unsealed affidavits may reveal investigative methods or facts that could result in action by a target that might diminish the amount of assets available for seizure (such as identification of a wallet address or specific cryptocurrency private key), destruction or complication of evidence (such as the deletion of logs or destruction of other digital

---

https://news.bitcoin.com/chainalysis-says-theyve-found-the-missing-1-7-billion-dollar-mt-gox-bitcoins/.

evidence), or worse.

4. Protective orders

Prosecutors may also consider filing a motion for a protective order to prevent public disclosure of sensitive law enforcement techniques provided by private companies, trade secrets, and other proprietary commercial information, including algorithms that are not relevant to the government's proof or the defense. In addition, consider whether to seek a protective order that would prevent public access to the specific proprietary information after a defendant is permitted to use it in their defense. Before doing so, consult with CCIPS or an NSD attorney about the implications of seeking such an order on the defendant's right to public trial under the Sixth Amendment of the U.S. Constitution.

Protective orders may be needed in cryptocurrency cases to address the company's other businesses with the government from detailed disclosure, trade secrets, or other information that could cause unnecessary damage to the company or national security.

V. Organizations' use of cryptocurrency in national security matters

In the case of terrorist organizations, cryptocurrency is still not the preferred method to transfer value. Instead, the long tradition of using hawalas remains a favored method of providing terrorists support, along with the use of commercial money transfer businesses. The difficulties in cashing out cryptocurrency in conflict regions contributes to the slow adoption of cryptocurrencies by terror groups.

Prosecutors, however, may see cases in which individual terror supporters are using cryptocurrency to crowd-fund a terror operation or to purchase servers or other computer infrastructure for hacking or extremist messaging.

Several nations under U.S. Department of Treasury sanctions have proposed the development of new cryptocurrency in an effort to undermine the dollar and thereby diminish the efficacy of sanctions.[77]

---

[77] Tony Spilotro, *Iran is Preparing National Rial-Backed Cryptocurrency to Evade US Sanctions*, NEWSBTC (Aug. 28, 2018), https://www.newsbtc.com/2018/08/29/iran-is-preparing-national-rial-backed-cryptocurrency-to-evade-us-sanctions/; Morgan Wright, *As Iran Turns to Bitcoin and Its Own Cryptocurrency to Avoid Sanctions, Maybe It's Time to Build Another Stuxnet*,

As the above-referenced indictment in the Russian election interference case demonstrates, cryptocurrency can be used by state actors and proxies to conceal purchases of infrastructure to be used in espionage or influence campaigns.

VI. Overlap with traditional criminal investigative techniques

A. Search and seizure

The first step to seizing virtual currency involves ascertaining the location of virtual currency private keys. The keys may be stored locally on a target's device or in physical form, in which case the agents should endeavor to locate them during the execution of a search warrant. Alternatively, the target may store virtual currency in accounts at virtual currency exchanges or at other remote locations.

If the funds are stored locally by the target, prosecutors should obtain a seizure warrant covering the premises and devices where the private keys are located. This is frequently accomplished by including authority to seize cryptocurrency within Attachment B of a Rule 41 search and seizure warrant.[78] If the funds are located overseas, consult with OIA, as an MLAT will likely be required.

If the funds are indeed stored locally, agents should be aware that they may be held in both physical and electronic form. Warrants should be drafted accordingly. Investigators should look for files or apps associated with cryptocurrency, as well as alphanumeric strings fitting the parameters of a cryptocurrency public or private key. Keys may be stored as QR codes or printed on paper as "paper wallets." Users may also back up their entire wallet with the use of root keys or recovery seeds, typically a series of short words listed in a particular order.

Investigators should also be mindful of the possibility of contextual evidence that may help tie a target to the underlying activity or offer clues as to the location of criminal proceeds. In that vein, investigators should look for specialized software installed on the target's devices, such as the Tor browser, browser history indicative of visits to cryptocurrency services, and records of exchange accounts or

---

THE HILL (Aug. 19, 2018), https://thehill.com/opinion/technology/402477-as-iran-turns-to-bitcoin-and-its-own-cryptocurrency-to-avoid-sanctions.

[78] FED. R. CRIM. P. 41.

transactions paid in cryptocurrency, among others.

Regardless of the cryptocurrency or wallet type, upon execution of a search and/or seizure warrant, the cryptocurrency should be moved to an agency-controlled wallet. It should then be held in "cold storage," that is, in a secure offline device, until it is transferred to a United States Marshals Service (USMS) wallet (see section VII, *infra*). If the seizing agency has difficulty accessing the cryptocurrency for seizure, it should work with the owner or contact CCIPS for assistance.

VII. Pre-seizure planning and forfeiture

A. Valuation

Cryptocurrency seizures with a value of more than $500,000 must be forfeited judicially rather than administratively.[79] The value is assessed on the date of agency seizure. After seizure, some wallets receive additional coins that may not be covered by the original seizure warrant. Establishing the value at the real-time of the seizure will be critical to its success. The value of coins also fluctuates dramatically. To explain changes in value that appear to throw off the link between the amount of cryptocurrency in a wallet and the transactions at issue in the charges, a record of the value at seizure should be part of the attribution and audit trail. Real-time and historical cryptocurrency exchange rates can be found online.[80]

B. Custody and liquidation

Each seizing agency should have a wallet or address for temporary storage of seized cryptocurrency prior to the transfer of custody to the USMS. Agencies typically set up one or more wallets for each seizure. Upon seizure of cryptocurrency, or prior to the seizure if circumstances allow, the seizing agency should request a cryptocurrency wallet or address from the USMS for transfer of the cryptocurrency. Cryptocurrency should be transferred either immediately after the seizure or at the conclusion of the case, depending on the individual agency's custodial policy.

---

[79] *See Policy Manual: Asset Forfeiture Policy Manual* (2016), ch. 2, sec. II.A, https://www.justice.gov/criminal-afmls/file/839521/download.

[80] COINBASEPRO, https://www.gdax.com/trade/BTC-USD (last visited Nov. 14, 2018); COINMARKETCAP, https://coinmarketcap.com/ (last visited Nov. 14, 2018).

In most cases, because of the risks that early conversion may pose, cryptocurrency should be kept in the form it was seized and not liquidated (that is, converted to fiat currency or other cryptocurrency) until a final order of forfeiture is entered or an administrative forfeiture is final. Agencies or prosecutors may, however, seek an order for the interlocutory sale of cryptocurrency at the request and/or consent of all parties with an ownership interest. Consultation with MLARS is required prior to any pre-forfeiture conversion or seeking an order for interlocutory sale of cryptocurrency.

Any liquidation of cryptocurrency should be executed according to established written policies of the seizing agency and the USMS. Currently, liquidation occurs via a periodic auction conducted by the USMS. Although the USMS can assume custody of and sell via auction many types of cryptocurrency, their ability to take and liquidate some coins is limited.

Prosecutors should be aware that a federal agency must follow all approval requirements for federal retention of forfeited property. Property under seizure and held pending forfeiture may not be used for any reason by government or contractor personnel, including for official use, until a final order of forfeiture is issued.[81] This prohibition is separate and apart from operational security issues implicated by putting cryptocurrency back into official use. Prosecutors and investigators may contact the USMS complex assets unit or MLARS for guidance regarding disposition of any alternative cryptocurrencies (for example, cryptocurrency other than Bitcoin) for which the USMS does not yet have a process in place to take custody or liquidate via auction.

VIII. International issues

A. Undercover operations and convincing a defendant to travel to a third country may be illegal in some countries and require OIA permission

Nothing establishes attribution better than an undercover operation that leads to an actual person to charge, especially if that target can be convinced to travel to a place where they can be taken into custody.

---

[81] *See Policy Manual: Asset Forfeiture Policy Manual* (2016), ch. 6, sec. IV, https://www.justice.gov/criminal-afmls/file/839521/download.

Often defendants in cryptocurrency-related cases are located in at least one or more foreign countries. Sometimes a defendant will have to be convinced to travel to a third country that is not the United States. Some of those countries may prohibit the use of undercover law enforcement activities within their borders, or forbid the arresting of targets without the involvement of two or three sets of government officials. For that reason, convincing a target or defendant to travel to a third country for an arrest requires careful coordination with OIA. OIA can also assist in explaining any prohibitions on undercover operations, treaties, and memoranda of understanding with the foreign country that may be relevant to the case.

B. Anticipating MLAT or other requests across one or multiple nations

Because exchanges and servers used in cryptocurrency cases may be located all over the globe, prosecutors should make sure they anticipate the possible need to use multiple MLAT requests or other established systems for requests and plan accordingly. A central feature of this planning involves early and careful coordination with OIA to allow for time to receive the information back from other countries.

C. Embedded national security risks where nation states involved, and other scenarios

Many cases can present national security concerns because of the nations that are involved in the criminal activity, or because particular individuals in those nations are acting against the national security interests of the United States. These concerns can also arise where the targets of the investigation are state actors, such as military or intelligence agents, or serve as proxies of a foreign government. Prosecutors should not assume that their knowledge of any particular country will suffice to guide them in managing these concerns. National security risks may only surface when a prosecutor discusses national security concerns with the investigative agents in their case, OIA, or the NSD. Prosecutors should work toward at least one person on the prosecution team itself holding the appropriate security clearance to review any classified information that might be relevant to the case.

IX. Sections for coordination and assistance

A. CCIPS

CCIPS advises on a range of cryptocurrency-related issues, including those that arise from the search and seizure of electronic evidence and those pertaining to the use of certain blockchain analysis tools.

B. MLARS

In 2017, MLARS established a Digital Currency Initiative. The program, serviced by a full-time Digital Currency Counsel, provides legal support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency-related prosecutions and forfeitures, to include:

- Expanding and implementing training to encourage and enable more investigators, prosecutors, and Department of Justice agencies to pursue such cases;
- Developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture;
- Advising Assistant United States Attorneys and federal agents on complex questions of law related to cryptocurrency to inform charging decisions and prosecutorial, seizure, and forfeiture strategies, particularly as relating to money laundering activities.

C. NSD

Consultation with NSD is helpful, and sometimes required, in cryptocurrency-related cases with a national security component. In cases involving possible espionage, foreign hacking, unlawful transfers of classified information, or violations of sanctions or export controls, the Counterintelligence and Export Control Section (CES) should be consulted and can provide assistance. If a case involves material support or funding of terrorists, the Counterterrorism Section (CTS) should be consulted and can provide valuable expertise. In some cases, clearance may be required.[82]

Any case that has a national security component may require

[82] JUSTICE MANUAL § 9-90.200.

additional due diligence with the intelligence community, which requires NSD Sections to become involved, and may require additional effort to de-conflict the ongoing investigation.

D. OIA

The OIA must be consulted in any case that involves investigation or acquisition of evidence of information from a foreign country. Advanced coordination with OIA must occur in cases where law enforcement seeks to lure an individual or desires to conduct undercover operations overseas.

E. Regulatory and civil enforcement agencies

There are hazards inherent in prosecutors reaching out to any regulatory agency, such as FinCEN, the SEC, or the Commodities Future Trading Commission. These include the possible disclosure of information protected under Federal Rule of Criminal Procedure 6(e) and the many legal issues involved in parallel proceedings.

Prosecutors should familiarize themselves with the cryptocurrency rules created by regulatory agencies by viewing their regulations and relevant guidance and contacting the NSD or MLARS within the Criminal Division for assistance with any risks presented by working with these agencies.[83]

About the Authors

Michele R. Korver is the Digital Currency Counsel in the Criminal Division's Money Laundering and Asset Recovery Section, serving as a subject matter expert for the Department of Justice on prosecutions and forfeitures involving cryptocurrency. Michele has served as an Assistant United States Attorney in the Miami, Florida, and Denver, Colorado, United States Attorney's Offices, where she investigated and prosecuted hundreds of violations of federal criminal law in U.S. courts.

C. Alden Pelker is a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice, where she specializes in the

---

[83] FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/ (last visited Dec. 7, 2018); SEC. & EXCHANGE COMM'N, https://www.sec.gov/ (last visited Dec. 7, 2018); U.S. COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/ (last visited Dec. 7, 2018).

investigation and prosecution of complex cyber criminal schemes involving cryptocurrency. She previously served as an intelligence analyst for the Federal Bureau of Investigation.

Elisabeth Poteat is a trial attorney in the Counterterrorism Section of the National Security Division of the United States Department of Justice. She served as an Assistant United States Attorney for the District of Columbia for over a decade.